REMARKS

Applicant respectfully requests reconsideration of the present application in view of the foregoing amendments and in view of the reasons that follow.

Claim 20 is currently being amended.

This amendment adds, changes and/or deletes claims in this application. A detailed listing of all claims that are, or were, in the application, irrespective of whether the claim(s) remain under examination in the application, is presented, with an appropriate defined status identifier.

After amending the claims as set forth above, claims 13-24 are now pending in this application.

In the Final Official Action of September 19, 2005, the Examiner rejected claim 20 under 35 U.S.C. § 112, second paragraph as being indefinite due to potential ambiguity involving whether "content" or a "menu application" is intended to be stored at a server. In response to this rejection, Applicant has amended claim 20 to clarify that it is the content that is stored at the server. In making this amendment, Applicant notes that the amendment is being made for clarification purposes only and is not intended to narrow the scope of the claim in any way.

The Examiner rejected claims 13-24 under 35 U.S.C. § 103(a) as being unpatentable over UK Patent Publication No. 2,349,548A, in the name of Roke Manor Research Limited (Roke Manor), in view of UK Patent Publication No. 2,344,491, in the name of Red Fig Limited (Red Fig). Applicant respectfully traverses these rejections for the reasons outlined below.

The Examiner has asserted that, with regard to claim 13, the Roke Manor teaches a system where a mobile device is permitted to contact a network operator so that software is sent to a subscriber site. The Examiner has apparently used this position to assert that the Roke Manor reference teaches a system where, in response to user selection of a direct download link, the radio communication device is controlled to transmit a signal to connect to

the server. Applicant disagrees with this position. In fact, even a cursory reading of the Roke Manor reference shows that the response to a user selection of a service is not to connect to the server. Instead, Page 6, lines 6-7 of Roke Manor unequivocally states that, upon the selection of a direct download link, the response of the device is to listen for the relevant Java class to be broadcast. It is only after the relevant class is detected that any contact will be made. In contrast, the present invention as described in claim 13 and its respective dependent claims is much more proactive. In claim 13, contact is made by the device in response to the user selection via the browser application, not in response to actions by the server. This is substantially different from the Roke Manor reference, where the response to the user selection of a link, the response is only to listen.

With regard to the Red Fig reference, the Examiner has noted that this reference teaches the browsing of the Internet using a mobile telephone so as to obtain variable data for HTML pages. However, the Red Fig reference does not teach a system where, in response to the action of a direct download link from a menu application, a browser application is caused to respond with retrieving the requested material. Therefore, even if the Red Fig reference were to be combined with the Roke Manor reference, the resulting system still would not teach the use of a direct download link from a menu application in order to cause a browser action to occur.

Because the Roke Manor reference (as well as the Red Fig reference) do not teach these features, Applicant submits that claim 13 and its respective dependent claims are patentable over the prior art. Additionally, as these features are also described in independent claims 14, 17, 18, and 19 and their respective dependent claims, Applicant submits that this element is missing from the Roke Manor and Red Fig references with respect to these claims as well.

In addition to the above, Applicant also asserts that neither the Roke Manor reference nor the Red Fig reference teaches or even suggests an authentication or validation process of the type specifically required by claims 13-16, 20 and 23. More particularly, and particularly with regard to claim 20, these claims require an authentication or validation process so as to

determine whether or not the downloaded content is from a trusted server. Neither of the cited prior art reference teaches this feature.

In the September 19, 2005 Action, the Examiner asserted that, by receiving an authentication code, the Roke Manor device "inherently" can determine whether the server is correct or valid because, in the Examiner's view, "only the correct 'server' for the Roke Manor device's software would have the correct authentication code." This argument is incorrect in several respects. In the case of the Roke Manor reference and as discussed on page 6 thereof, the authentication code being provided to the electronic device is only used to enable the software that the server itself provided. It is not used to authenticate the server as a trusted server. Untrusted servers can and often will provide software containing worms, viruses, and other malicious code that can adversely affect devices which download the software. Paragraph No. 45 of the present application discusses the concept of a trusted server and further elaborates on this point:

> A trusted server is one that the mobile phone recognises is a server authorised to provide content for download to the mobile phone, and this may be on the basis of information pre-loaded, flashed or even downloaded to the phone's memory, and may be implemented for example in the form of a look-up table. Advantageously, the invention provides a safeguard against the content crashing the phone.

The Roke Manor system does not address the issue of a trusted server. Instead, the Roke Manor server does nothing more than permit the downloading device to use the software provided by the server itself. In fact, if the Roke Manor system were used by a malicious programmer, the programmer would simply have to create his "own" authentication code to be transmitted along with his malicious software. Using the Examiner's logic, a user downloading this software should have no problem inherently "trusting" this software because he received the "correct" code. However, this software clearly cannot be trusted. The present invention as described in claim 20, however, does address this issue through the validation data required by independent claim 20, and Applicant submits that the prior art completely fails to identify this issue, much less address it.

In addition, the validation process that occurs in claims 13-16 and 21-24 is entirely different from the "authentication" process described in the Roke Manor reference. In the Roke Manor reference, the authentication code described on page 4 is used to grant content access to the client device. ("The network operator 12 then transmits an authentication code to the subscriber 16 via a GSM base station 18 which enables the Java class software to run.") In other words, this code is used to validate the client device. In contrast, the validation process described in claims is 13-16 and 21-24 is to validate the server. For example, claim 13 is clear that the validation data is associated with the content so as to be identifiable by the authentication means as originating from the server. Like claim 20, the purpose of this function is to provide safeguards against downloads from potentially harmful devices. The authentication mechanism of the Roke Manor reference does not perform this function, instead only permitting the server (whether trusted or not) to control where its content is used.

For the above reasons, Applicant respectfully submits that claims 13-24 are patentable over the cited prior art.

Applicant believes that the present application is now in condition for allowance. Favorable reconsideration of the application as amended is respectfully requested.

The Examiner is invited to contact the undersigned by telephone if it is felt that a telephone interview would advance the prosecution of the present application.

The Commissioner is hereby authorized to charge any additional fees which may be required regarding this application under 37 C.F.R. §§ 1.16-1.17, or credit any overpayment, to Deposit Account No. 06-1450. Should no proper payment be enclosed herewith, as by a check being in the wrong amount, unsigned, post-dated, otherwise improper or informal or even entirely missing, the Commissioner is authorized to charge the unpaid amount to Deposit Account No. 06-1450. If any extensions of time are needed for timely acceptance of papers submitted herewith, Applicant hereby petitions for such extension under 37 C.F.R. §1.136 and authorizes payment of any such extensions fees to Deposit Account No. 06-1450.

Respectfully submitted,

Date January 18, 2006

By _____

FOLEY & LARDNER LLP
Customer Number: 27433
Telephone: (312) 832-4500
Facsimile: (312) 832-4700

Marshall J. Brown
Attorney for Applicant
Registration No. 44,566

G. Peter Albert, Jr.
Attorney for Applicant
Registration No. 37,268